

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de la pile TCP sous Solaris

---

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>  
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2002-AVI-237>

---

### Gestion du document

Référence	CERTA-2002-AVI-237
Titre	Vulnérabilité de la pile TCP sous Solaris
Date de la première version	28 octobre 2002
Date de la dernière version	–
Source(s)	Bulletin de sécurité #48209 de Sun
Pièce(s) jointe(s)	Aucune

TAB. 1 – *gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

## 1 Risque

Déni de service (consommation des ressources).

## 2 Systèmes affectés

Les versions suivantes de Solaris pour Sparc et Intel sont vulnérables :

- Solaris 2.6 ;
- Solaris 7 ;
- Solaris 8.

## 3 Résumé

Il est possible de consommer toutes les ressources du système à distance grâce à l'envoi massif de paquets TCP sur la machine cible.

## **4 Description**

Un utilisateur mal intentionné peut engendrer un déni de service en envoyant massivement des paquets TCP ACK (Acknowledge) sur la machine victime.

Celle-ci emploiera trop de ressources lors du traitement de la réponse à ces paquets (réponse par des paquets TCP reset (RST)) pouvant entraîner un gel de la machine.

## **5 Contournement provisoire**

Installer un firewall à états sur le système ou en amont du réseau à protéger.

## **6 Solution**

Consulter le bulletin de sécurité du système concerné (voir paragraphe Documentation) afin de connaître la disponibilité des correctifs.

## **7 Documentation**

Bulletin de sécurité #48209 de Sun :

<http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F48209>

## **Gestion détaillée du document**

**24 octobre 2002** version initiale.